(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 July 2005 (14.07.2005)

PCT

(10) International Publication Number
WO 2005/062951 A3

(51) International Patent Classification[7]: H04L 9/08, 9/00

(21) International Application Number:
PCT/US2004/043416

(22) International Filing Date:
22 December 2004 (22.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03293294.9 23 December 2003 (23.12.2003) EP

(71) Applicant *(for all designated States except US)*: **MOTOROLA, INC., A CORPORATION OF THE STATE OF DELAWARE** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KELLIL, Mounir,** [FR/FR]; 2, rue du Bearn, BP 303, F-94550 Chevilly Larue (FR). **JANNETEAU, Christope Jacques Phillippe,** [FR/FR]; 10, rue Auguste Renoir, F-78390 Bois D'Arcy (FR). **OLIVEREAU, Alexis,** [FR/FR]; 11, Rue Maurice Bertaux, F-91120 Palaiseau (FR).

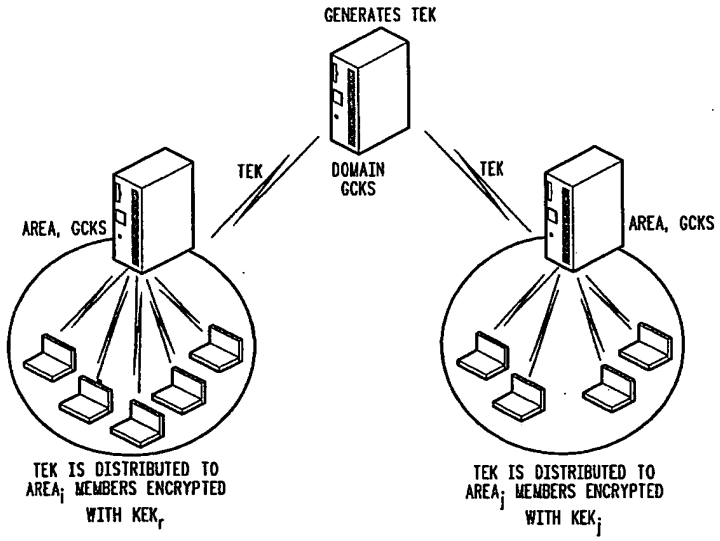
(74) Agent: **PACE, Lalita W., GTSS Pate**; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: REKEYING IN SECURE MOBILE MULTICAST COMMUNICATIONS



(57) Abstract: A method of inter-area rekeying of encryption keys in secure mobile multicast communications, in which a Domain Group Controller Key Server (Domain GCKS) distributes Traffic Encryption Keys (TEK) to a plurality of local Group Controller Key Servers (local GCKS), and said local Group Controller Key Servers forward said Traffic Encryption Keys, encrypted using Key Encryption Keys (KEKi, KEKj) that are specific to the respective local Group Controller Key Server (local GCKSi, GCKSj), to group members, said local Group Controller Key Servers (GCKSi, GCKSj) constituting Extra Key Owner Lists (EKOLi, EKOLj) for group key management areas (areai, areaj) that distinguish group members (MMi, MMj) possessing Key Encryption Keys (KEKi, KEKj) and situated in the corresponding group key management area (areai, areaj) from group members (MMij) possessing Key Encryption Keys (KEKi) that were situated in the corresponding group key management area (areai) but are visiting another area (areaj).

WO 2005/062951 A3

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
17 November 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.